CONTRABAND PHONE TASK FORCE STATUS REPORT

by
CTIA and ASCA
April 26, 2019

In February 2018, Federal Communications Commission Chairman Ajit Pai convened a diverse group of stakeholders – state corrections officials, solutions providers, public safety experts, the wireless industry, and the U.S. Department of Justice Bureau of Prisons – to address how best to leverage technological solutions to combat contraband devices in correctional facilities. Chairman Pai called on meeting participants "to determine the most effective, affordable, and safe ways to address this problem—that is, to stop the threat of contraband cellphones without causing harm to legitimate wireless users."[1]

At the meeting, CTIA proposed to stand up a Task Force to examine potential technological, legal, and administrative challenges and solutions to combat contraband devices while accounting for the interests of legitimate wireless users.[2] Joined by the Association of State Correctional Administrators (ASCA) and the Bureau of Prisons (BOP), CTIA launched the Contraband Phone Task Force in April 2018. This Task Force Report (Report) provides a summary of the Task Force's activities to date in the following areas:

(1) Coordination and collaboration among wireless service providers and corrections officials to identify contraband phone challenges and potential solutions;
(2) Establishment of a Testbed for the technical assessment of Contraband Interdiction System (CIS) technologies (Attachment A to this Report provides a detailed analysis of the findings of the Testbed and recommended best practices for deploying CIS technologies based on lab and field test observations);
(3) Implementation of state-level court order processes to enable wireless carriers to disable cellular service to contraband devices;
(4) Use of the wireless industry's Stolen Phone Database to deny service to contraband phones across multiple cellular networks; and

---

[1] FCC News, Chairman Pai Convenes Meeting to Discuss Combatting Contraband Wireless Devices in Correctional Facilities (Feb. 7, 2018), https://docs.fcc.gov/public/attachments/DOC-349082A1.pdf.

[2] The Testbed described below and the attached report address technical solutions to reduce the use of contraband devices, although there are also a number of non-technical solutions to reduce or prevent the unlawful possession and use of contraband devices in correctional facilities.

(5) Review of the possibilities and challenges of geofencing capabilities as a contraband interdiction solution (Attachment B to this Report summarizes how geofencing could operate in a correctional facility setting and CTIA's related views on legal and privacy issues).

Members of the Task Force have forged a strong working relationship throughout the Task Force process (Attachment C to this Report identifies the Contraband Phone Task Force's member organizations). Following the most recent Task Force meeting in January 2019, CTIA and ASCA noted the following in a joint statement: "We continue to be encouraged by the collaboration between corrections officials and the wireless industry to address this important issue."[3] Attachment D to this Report is a statement issued by ASCA reinforcing that "serious crimes are being orchestrated on [ ] smuggled devices," that "the partnership between CTIA and ASCA has been productive and appreciated," and that state correctional institutions "need access to the full complement of tools" to help stop contraband devices.

We commend Congress and the Federal Communications Commission (FCC) for their ongoing commitment to combat contraband devices in correctional facilities, and we applaud Congress' recent decision to incorporate $2 million "for grants to States and units of local government to deploy managed access systems to combat contraband cell phone use in prisons" in recently enacted appropriations legislation.[4] Task Force members appreciate Congress' decision to dedicate funding for this important initiative.

Finally, we note that this report reflects the beginning of the Task Force's initiative, not its conclusion. Participating industry representatives and corrections officials will continue to meet and to work collaboratively on solutions to address this critical public safety issue. As interdiction technology solutions continue to emerge, and as corrections officials' needs and experiences evolve, all parties will need to work cooperatively to assess both the effectiveness of new technologies and their impact on legitimate users. We are committed to doing that.

[3] CTIA and ASCA Statement on January 10, 2019 Contraband Phones Task Force Meeting (Jan. 10, 2019), https://www.ctia.org/news/ctia-and-asca-statement-on-january-2019-contraband-phones-task-force-meeting.

[4] *See* Pub. L. 116-6.

I. Task Force Activities.

In April 2018, CTIA launched the Task Force with ASCA to coordinate an in-depth examination of potential technological, legal, and administrative solutions to contraband device use in correctional facilities. CTIA and wireless carrier members have provided the funding for the Task Force's work and, with ASCA and BOP, have supported the Task Force by making their facilities available for field testing and the commitment of substantial amounts of their experts' time.

The Task Force is comprised of representatives from CTIA, wireless carriers, ASCA, state corrections officials from Alabama, Arkansas, California, Indiana, Mississippi, Oklahoma, South Carolina, Tennessee, and Texas, and BOP. It also has interfaced and solicited input from the CIS vendor community.

The Task Force has held four face-to-face meetings and has engaged in a variety of activities since its launch. Relationships developed through the Task Force have also led to additional meetings and calls to discuss state-specific issues related to contraband phones.

The first Task Force meeting, held in April 2018, formally initiated the Task Force and began a carefully executed process of determining the scope and manner of testing CIS technologies.

Using the input collected during the April Task Force meeting and the discussions that followed, CTIA retained the Virginia Tech Applied Research Corporation (VT-ARC) to develop a CIS Testbed and conduct technical assessments of different CIS technologies. Dr. Charles Clancy, an internationally recognized expert in wireless security and Bentley Professor of Cybersecurity, Electrical and Computer Engineering at Virginia Tech, led the VT-ARC team.

The Task Force held a CIS vendor workshop on June 13 and 14, 2018 to foster consideration of a broad range of CIS technologies in the development of the Testbed. The Testbed then solicited applications from all participating CIS vendors to participate in the testing. Vendors that participated in the Testbed paid a nominal fee for the testing process.[5] Although the testing process initially

[5] The fee, $10,000, did not cover the costs of the testing but was intended to ensure that any CIS solutions put forward in the Testbed were sufficiently advanced, mature, and commercially available solutions. The fee was discussed in depth by Testbed members at the June Task Force meeting and it was agreed that the $10,000 fee was necessary to ensure that the Testbed did not get overwhelmed with CIS solutions that were not ready to be tested in a live-environment.

was expected to take 12-16 months, CTIA and the VT-ARC team expedited the timeline to eight months at the request of corrections officials on the Task Force.

In parallel with the Testbed activity, Task Force members also made significant progress on legal and administrative measures to combat contraband device use. Specifically, based on a model court order developed by CTIA, some state corrections and law enforcement agencies have filed for and received court orders directing carriers to disable specific contraband devices.[6] Carriers regularly engaged their internal law enforcement support teams with these agencies to address practical questions and refine the process of obtaining and executing court orders. In addition, CTIA worked with other stakeholders to include and list contraband devices in the industry's existing Stolen Phone Database, which complements the court order process and prevents device operation regardless of network or carrier.

The Task Force held its second face-to-face meeting in June 2018 and its third meeting in September 2018. During the June meeting, Task Force members and Dr. Clancy discussed key considerations and take-aways from the CIS vendor workshop. In September, Task Force members toured VT-ARC's Testbed facility and viewed demonstrations of the technologies themselves.

The most recent Task Force meeting was held in January 2019 at ASCA's Winter Meeting in New Orleans. At the meeting, VT-ARC briefed Task Force members on the Testbed results and recommended best practices for deploying CIS technologies in correctional facilities. Members also discussed geofencing technologies as a potential method to identify and disable service to contraband devices.

II. Testbed Assessment of CIS Technologies.

CTIA engaged VT-ARC in April 2018, and since then VT-ARC has been leading the Testbed process on behalf of the Task Force.

Development of the Assessment Process. The Task Force and VT-ARC conducted extensive outreach to CIS vendors to exchange information about the Testbed and the Task Force's broader objectives, including during the June 2018 vendor workshop. Twelve CIS technology vendors attended the workshop, and nearly all presented technical details of their systems as well as information

[6] The identification of contraband devices for purposes of court orders requires the installation of a contraband interdiction system.

about cost and current deployments.[7] These presentations illustrated the diversity of technical approaches to contraband device interdiction. After the workshop, VT-ARC invited all twelve vendors to submit their systems for evaluation in the Testbed.

Three CIS solutions – two managed access systems (MAS) and one jamming solution – accepted this invitation.[8] The two MAS solutions that were tested consisted of multiple software defined radios that interdicted cellular communications by overpowering signals from surrounding commercial cellular networks, thus causing cell phones in the MAS coverage area to attach to the MAS network. The jamming solution included in the Testbed emitted RF signals in five frequency bands to overpower downlink signals from surrounding cellular networks.

In parallel with the vendor selection process, VT-ARC developed rigorous test protocols for lab and field conditions. The testing proceeded in two main stages. First, VT-ARC evaluated all three systems under closely controlled laboratory conditions.[9] The laboratory tests were based on simulated 2G, 3G, and 4G cellular core networks with support for voice service, text messaging, web browsing and File Transfer Protocols. VT-ARC tested a collection of unlocked phones that are representative of phones seized in correctional facilities. VT-ARC then field-tested the two MAS systems. One test occurred at Lee Correctional Institution in Bishopville, South Carolina, and the other at Mark W. Stiles Unit in Beaumont, Texas. These tests provided insight into how MAS technologies perform under real-world conditions. With regard to jamming technology, the FCC has determined that 47 U.S.C. § 333 prohibits state and private operation of jamming devices that block authorized radio communications, so no field testing of jamming operations was conducted.[10]

---

[7] The participating vendors were CellAntenna, Corrections.com, Securus Technologies, Global Tel Link, Harris, J3Technologies, Metrasens, NCIC, Prelude Development, SafeCell Technologies, ShawnTech, and Tecore.

[8] Several vendors declined to submit their systems for testing, citing, among other reasons, the need to further develop their systems before testing, and incompatibility between their systems and the Testbed's capabilities.

[9] The laboratory testing was conducted in a controlled, cabled environment with cellphones in an RF Test Enclosure. The jammer tests were performed in a walk-in Faraday cage.

[10] *See* Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, FCC GN Docket No. 13-111 (released May 1, 2013), at ¶ 19 (stating that the Communications Act "prohibits any person from willfully or maliciously interfering with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government" and "jammers are not permitted under the Commission's rules," citing 47 U.S.C. § 333).

Overview of Test Results. The Testbed produced detailed insights into the performance of the three solutions (although one solution, jamming, was only tested in a laboratory setting due to the legal prohibitions referenced above). Testing outcomes are highly dependent on the specific technologies under assessment, their configurations, and conditions of surrounding cellular networks, and it is essential to view the results in this light. Further, laboratory testing provided a circumstance in which environmental variables and equipment configurations were closely controlled, making experiments repeatable and allowing comparisons across different CIS solutions. The laboratory testing environment, however, did not replicate many of the features and variables of a "live" correctional facility environment – nor was that the purpose of this kind of testing; rather, the Task Force engaged in field testing to address deployments in real world conditions. Given FCC precedent finding that 47 U.S.C. § 333 prohibits private entities such as VT-ARC from operating jamming devices, field testing did not occur for the jamming solution that participated in the Testbed. Further testing in both laboratory and field conditions, and in some cases collaboration among service providers, BOP, the FCC, and other stakeholders (including the Department of Commerce and the National Telecommunications and Information Administration (NTIA)) would be needed to more fully assess the effectiveness of the technologies and the potential interference with legitimate users.

MAS. By way of background, MAS solutions effectively overpower the coverage of surrounding commercial cellular networks within a specific physical area, using antenna placement and power settings designed to keep their RF signals confined within specific geographic areas, such as the perimeter of a correctional facility. Successful contraband interdiction, while minimizing disruption to surrounding cellular networks, requires careful planning and design and ongoing monitoring, service, and support of a MAS installation. MAS providers routinely obtain spectrum leases from the surrounding cellular network licensees at little or no cost and receive streamlined processing at the FCC.

The two MAS solutions in the Testbed succeeded in interdicting communications from contraband devices over simulated and actual cellular networks. The effectiveness of the MAS solutions depended on the power of the interdiction system's signal relative to the surrounding commercial cellular networks as well as their coverage of frequency channels used by contraband devices. In its laboratory testing, VT-ARC incrementally decreased the power of the MAS networks to test devices attached to the simulated cellular network, revealing a "crossover" point at which actual contraband phones would evade interdiction.

In its field tests, VT-ARC observed that both MAS solutions were successful in blocking unauthorized communications in most areas in the correctional

facility campus. However, at one of the field test sites, the MAS was weak or did not fully block communication attempts from certain areas of the facility, which were mostly under construction and unoccupied during testing. In addition, signals from both MAS solutions were generally contained within the correctional facilities, suggesting that the systems posed little risk of interference to legitimate wireless users beyond the facilities' perimeters at the time of testing, although isolated instances of interference were reported at one of the test sites prior to testing.

VT-ARC noted that MAS solutions are not simply plug-and-play but involve initial upfront costs and ongoing monitoring and maintenance. For instance, some current MAS solutions depend, in part, on causing phones to switch to 2G, an approach that could become ineffective as 2G chips are phased out of devices. Cellular carriers' deployments of 5G also may require MAS solutions to cover additional frequencies. More generally, MAS systems require ongoing maintenance to detect changes in surrounding cellular networks, destruction of MAS equipment by inmates, or other issues that could affect MAS effectiveness. Finally, it has been reported that correctional staff onsite have issues with communicating with each other in certain areas of the correctional facility, particularly in areas where the MAS network would typically handover to the macro network and in locations within the facility with weaker coverage or in between MAS coverage zones. Some corrections officials also still have concerns for the cost of MAS technologies and practical maintenance issues, such as vandalism of equipment by inmates.

Jamming. The Testbed found that the one jamming solution tested was capable of denying service to contraband devices operating in frequency bands covered by the jammer under laboratory conditions.

Like MAS, a jamming solution must provide sufficient coverage to deny cellular service inside a correctional facility without interfering with wireless services outside the facility. Based on the one technology tested, achieving sufficient coverage of jamming signals within a correctional facility could require the installation of many jammers – up to one per inmate cell – and extensive, location-specific planning to achieve the desired coverage. However, the single jamming solution that was tested in the CIS Testbed was not necessarily representative of all possible jammers that may be considered for use in federal correctional facilities.[11]

Laboratory testing of the one jamming solution that participated in the Testbed indicated that a real-world deployment of this system could cause harmful interference with co-channel commercial wireless service outside a

[11] We are unaware of any current use of jammers in federal correctional facilities.

correctional facility (which may affect 9-1-1 calls and public safety communications on that spectrum). However, testing additional jamming solutions in both laboratory and field conditions could more fully assess the likelihood of harmful interference. VT-ARC also observed in laboratory testing that the tested jammer lacked external filtering and created significant out-of-band interference, potentially threatening communications on channels outside of carriers' commercial cellular networks. Further, the testing confirmed that contraband devices could successfully communicate on channels that the jammer did not cover (or covered with insufficient power).

VT-ARC also looked at the complexity and cost to install, configure, and maintain jammers, drawing assumptions from the one technology tested, to satisfy the dual requirements of sufficient coverage inside the correctional facility and avoiding harmful interference on the outside. Based on its assessment of the tested jamming solution, VT-ARC found that achieving the desired performance – particularly in urban areas, where the potential for unintended interference is the greatest – could require installations that resemble distributed antenna systems (like those used in MAS systems) in complexity. The amount of jamming equipment required – and thus one element of cost – is likely to increase in proportion to a correctional facility's size. In addition, cost is likely to be proportional to the complexity of a correctional facility's radiofrequency environment. Finally, as noted above with respect to MAS, changes in the cellular bands that carriers use as well as changes in correctional facility buildings could degrade jamming performance, particularly given the potential for out-of-band interference. Similarly, the ongoing assessment and maintenance that would be necessary to ensure that a jamming solution is performing as intended add further to cost. Taking all of these factors into account, and drawing conclusions from the one technology analyzed, VT-ARC concluded that the overall cost of this solution may approach that of a MAS installation. Careful field testing of further jamming solutions under the auspices of the federal government (and thus not subject to the jamming prohibition of 47 U.S.C. § 333 under FCC precedent) could help assess effectiveness as well as the risk of interference to legitimate wireless users. Any further testing should be conducted in conjunction with the nearby wireless service providers in order to meaningfully assess the impact on commercial networks and the risk of harmful interference to legitimate wireless users.

Best Practices for CIS Deployments. VT-ARC's report also provides several suggested guidelines and best practices for the operation of CIS solutions. The recommendations include technical, administrative, and physical security considerations for vendors, corrections officials, and wireless carriers, further highlighting the need for cooperation among stakeholders to address contraband device challenges.

Finally, the Task Force's in-depth examination of MAS technologies suggests a path toward a "MAS Evolved" approach that could be more effective, less complex, and less costly to implement than current MAS solutions. This approach could leverage collaboration between MAS vendors and carriers through various agreements, which could substitute for the RF coverage complexity inherent in today's MAS solutions within correctional facilities. Such an approach could make new MAS installations less costly and improve the ability to locate contraband devices in correctional facilities (though, as noted above, the move to 5G may necessitate a substantial redesign of the RF distribution network, for both jamming and MAS technologies).

III. Putting into Practice a Court Order Process

Some CIS solutions capture device identifiers from phones that attach to their networks, and the Task Force explored the use of court orders to require a carrier to discontinue service to identified contraband devices, thus protecting lawful users. This process ensures a high degree of accuracy in the list of contraband devices identified, is familiar to law enforcement and wireless carriers, helps enforce criminal laws relating to contraband phone use, and protects lawful users of wireless service. In short, a court order process encourages accurate identification of contraband devices and provides a level of oversight that is consistent with comparable law enforcement efforts.[12]

To address the risks of harm to legitimate wireless users, the process for disabling service should provide reasonable assurance that targeted devices are involved in prohibited uses *before* service is disabled without compromising the objective of addressing risks to law enforcement and the public from contraband devices. In addition, because service termination essentially involves the activity of third parties (i.e., wireless carriers) in assistance to law enforcement, a formal legal process to govern service termination is appropriate.[13] A court order process – in which a judge requires a carrier to disable service to one or more contraband devices – is the most appropriate vehicle to provide these safeguards.[14]

CTIA developed and shared with the Task Force a model court order template that combines speed, scalability, and flexibility and leverages

[12] *See, e.g.*, CTIA Reply Comments, GN Docket 13-111, at 3-5 (filed July 14, 2017).

[13] *See* CTIA Reply Comments, GN-Docket 13-111, at 3 (filed July 14, 2017); Letter from Patrick Donovan, CTIA, to Marlene H. Dortch, GN Docket No. 13-111, at 2-4 (filed January 23, 2018).

[14] *See* CTIA Reply Comments, GN Docket 13-111, at 3-5 (filed July 14, 2017).

correctional facilities' existing interdiction efforts.[15] A single request by a correctional facility or law enforcement agency for a court order can direct carriers to disable wireless service to many devices at once and will include the identified devices in the industry's Stolen Phone Database discussed below, thereby allowing the process to scale up with the number of contraband phones that correctional facilities identify. In addition, the court order template has proven to be flexible enough to adapt to specific jurisdictions.

Law enforcement laws and procedures vary between states, so the template and its underlying concepts must necessarily be adapted accordingly. Nevertheless, as a result of the efforts of the Task Force, at least five states have used some form of the court order process to direct wireless carriers to disable wireless service to contraband devices. The Task Force has helped to bridge the gap between CTIA's model court order and the legal and procedural requirements of specific jurisdictions. For example, in California, officials from the Department of Corrections and Rehabilitation (CDCR) consulted with Task Force members to develop a California-specific implementation of the model court order process. For months, representatives of CTIA and the four national carriers participated in biweekly calls with CDCR officials to discuss the practical and legal considerations relevant to a court order process in California. In July 2018, California successfully applied for a warrant requiring the carriers to disable service to specific contraband phones located in a California correctional facility.[16] The warrants were served on carriers and processed through their own law enforcement support and response centers, which have also committed time, personnel and expertise to this effort. California officials subsequently obtained and served an additional set of warrants in November 2018, and another in February 2019, in which they ordered carriers to disable service to approximately 300 contraband phones.

CTIA and carrier representatives also worked closely with the South Carolina Department of Corrections to develop a process appropriate for that state. Corrections officials used this process to successfully apply for orders requiring carriers to disable service to specific contraband devices. As in California, carriers responded to these orders by disabling service to identified phones on their respective cellular networks. As an outgrowth of Task Force

---

[15] *See id.* at 3-6 (discussing how a court order process for contraband device service termination encourages accurate device identification, is adaptable to specific jurisdictions, and is consistent with processes governing private-sector assistance with law enforcement actions).

[16] *See* California Dept. of Corrections and Rehabilitation, Kern County affidavit calls for the termination of nearly 100 contraband cellphones (July 29, 2018), https://www.insidecdcr.ca.gov/2018/07/kern-county-affidavit-calls-for-the-termination-of-nearly-100-contraband-cellphones/ (reporting on the issuance of a warrant directing carriers to suspend and discontinue service to phones identified as contraband in the warrant application).

discussions, members continue to work with state officials to facilitate the court order process in South Carolina. Four other states – Georgia, Mississippi, Tennessee, and Indiana – have now also launched court order processes.

These promising initial efforts have also pointed toward ways to make it more efficient to obtain, serve, and comply with contraband device service termination orders. Task Force members plan to incorporate these lessons into further collaboration with member companies and corrections officials in California, South Carolina, and other states, to expand the use of this means of disabling service to contraband devices.[17]

IV. Use of the Stolen Phone Database to Extend the Reach of Court-Ordered Service Termination

The Task Force is also leveraging the Stolen Phone Database (SPD) to extend the effective reach of court-ordered service termination.[18] Specifically, whereas court orders are binding on specific carriers, by entering relevant device information into the SPD, the device becomes disabled across multiple wireless providers and networks. In this way, wireless service will not work even if an inmate replaces one SIM card with another from a different wireless carrier.

In an effort to provide an immediate means of including contraband devices in the SPD, CTIA has worked with the SPD administrator to develop a short-term solution that effectively includes contraband devices in the SPD. As a future step, the SPD infrastructure will establish a contraband device designation to enable enhanced reporting and recordkeeping on listed contraband devices.

V. The Possibilities and Challenges of Geofencing

As part of the January 2019 Task Force meeting, VT-ARC briefed members on carrier-based geofencing as a possible solution to prevent mobile devices from operating within the geographic boundary of correctional facilities. Today, geofencing is a theoretical concept and is not deployed as a CIS solution. Attachment B provides a summary of the VT-ARC description and identifies CTIA's review of legal and privacy issues surrounding a geofencing approach.

* * * * *

[17] *See, e.g.*, S.B. 2704, 2019 Reg. Sess. (Miss. 2019) (authorizing circuit courts to order carriers to disable service to contraband phones); H.B. 1237, 2019 Reg. Sess. (Miss. 2019) (same).

[18] Consumers can access information in the SPD through CTIA's Stolen Phone Checker, which is available at https://stolenphonechecker.org/spc/.

In 2019, the Task Force will continue to maintain and build on the collaborative, multi-faceted efforts that led to the results discussed in this report. The Task Force plans to hold several member meetings in the coming year. Task Force members have identified three substantive areas to address in 2019: (1) exploring technological approaches to improve MAS performance and potentially lower costs, dependent on MAS vendor decisions and feasibility assessments at the carrier level; (2) implementing permanent changes to the SPD to improve its support for contraband interdiction; and (3) expanding the use of court orders to terminate service to contraband phones.

The Task Force appreciates Chairman Pai's leadership on contraband phone issues. Identifying practical solutions to combat contraband device use requires not only technological, legal, and administrative approaches, but also collaboration among key stakeholders. The Task Force looks forward to continuing to work together to develop approaches that effectively disable service to contraband devices while at the same time protecting lawful users' interests in their wireless service.